Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 16 June 2003

Current Nationwide Threat Level is

For info click here
www.whitehouse.gov/homeland

Daily Overview

- U.S. Department of Agriculture reports ConAgra Poultry Company, an Athens, GA, establishment, is voluntarily recalling approximately 129,000 pounds of fresh chicken that may contain glass. (See item 8)
- Global Security Newswire reports that according to health officials and public health experts, efforts to prepare for a bioterrorist attack have enabled an effective response to this month's outbreak of monkeypox in the U.S. (See item 13)
- The Mercury News reports an 18−year−old hacker, who breached computers at Sandia National Laboratories and posted an anti−Israeli message on the Eglin Air Force Base Web site, was sentenced Thursday to a year and a day in federal prison. (See item 19)
- The Associated Press reports an eastern Washington state man, Richard Vialpando, has been arrested on federal charges of threatening to blow up Grand Coulee Dam. (See item 20)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 14, New York Times* — **Iraqi pipeline blast and fire are laid to sabotage.** An explosion occurred Thursday night along a major oil pipeline route in north−central Iraq and appears to have been an act of sabotage, according to a top Iraqi oil official. **"This is the first time we managed to know that it is sabotage," said Adel Qazzaz, the director general of Iraq's Northern Oil Company,** `which manages oil production in the large Kirkuk field. "There have

been fires before, but we thought those were because of seepage from old pipes." Reached by phone in Kirkuk, Qazzaz said he was informed this morning by colleagues in Beiji, an oil refining center about halfway between Kirkuk and Baghdad, **that an attack on a pipeline route had touched off an explosion. Three pipelines were affected, he said, and a fire is now burning at the site.** The pipelines carry oil for export to the Beiji complex, the largest in Iraq. **The explosion is the latest and among the clearest acts of sabotage against the Iraqi oil industry.** Thursday's explosion came just as the State Oil Marketing Organization, which oversees the export of Iraqi oil, announced the companies that would buy Iraq's first oil exports since the war, among them ChevronTexaco and France's TotalFinaElf.
Source: http://www.nytimes.com/2003/06/14/international/worldspecial /14PIPE.html

2. *June 12, Platts Global Energy News* — **Reactor pressure vessel bottom inspections may become routine. Inspections of reactor pressure vessel (RPV) bottoms may become the norm, with both the Nuclear Regulatory Commission (NRC) and the nuclear power industry moving in that direction.** Bill Bateman of NRC's Office of Nuclear Reactor Regulation told industry officials during a meeting on materials issues June 12, that the agency is considering requiring all units with fall outages to conduct bare metal inspections of the vessel bottoms. **STP Nuclear Operating Co. isn't expected to have determined by then the root cause of the bottom−originating leakage found at South Texas−1,** he said. Separately, the Electric Power Research Institute (EPRI) Materials Reliability Program (MRP) is recommending that all plants with bottom−mounted instrumentation nozzles perform visual inspections during future outages. **The industry group won't get into reinspection frequency until after the root cause at South Texas has been determined,** said MRP Chair Larry Mathews of Southern Nuclear. But he said such inspections might be called for at every outage. Alex Marion of the Nuclear Electric Institute said all plants have been asked when they would perform such inspections and what modifications might be needed. He said he expected to have answers in two weeks.
Source: http://www.platts.com/stories/nuclear2.html

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *June 13, Federal Computer Week* — **Army exercise puts communications technology to test.** As part of its continued efforts in the war on terrorism, the Army is testing its latest communications technology to ensure that secure connections are always available, whether on the battlefield or at home. **The exercise, known as Grecian Firebolt 2003, is being held at Fort Meade, MD, June 9−20. It is the world's largest peacetime communications exercise and it is designed to test new communication initiatives and systems against realistic scenarios.** The Army hopes that this exercise will ensure it is able "to provide a seamless network all across the board," said Maj. Gen. George Bowman, commander of the 311th

Theater Signal Command. **The exercise also enables the Army to test whether its systems are interoperable with other agencies, such as the Homeland Security Department and the Federal Emergency Management Agency.** The Army is conducting testing using the Defense Collaborative Tool Suite to communicate with federal agencies. DCTS is a set of commercial products intended to enable geographically separated users to chat, conduct videoconferences and share documents, slides and applications online.
Source: http://www.fcw.com/fcw/articles/2003/0609/web−firebolt−06−13 −03.asp

4. *June 13, Federal Computer Week* — **Homeland, Defense compatibility needs work.** More needs to be done to ensure compatibility between the Homeland Security Department and the Defense Department, according to Peter Verga, special assistant to the secretary of Defense for homeland security. In the wake of Sept. 11, 2001, DoD's role in helping first responders and directly defending the country has changed dramatically, Verga said June 12 at FCW Media Group's E−Gov 2003 conference in Washington, D.C. **One of the main problems that remains, Verga said, is the area of communications interoperability. "That is probably going to get solved in the near future," he said. "But we still have to overcome procedural, cultural, training and standardization barriers.** Beyond simple communications, getting the different agencies responsible for protecting the homeland to share data is a much larger hurdle to overcome. There is no plan to develop a true "enterprise architecture" to link DOD and DHS, but Verga said a meeting will take place next month to discuss how information can be shared. The meeting will include the Defense secretary's office, the Joint Forces Command, Northern Command and DHS.
Source: http://www.fcw.com/fcw/articles/2003/0609/web−verga−06−13−03 .asp

[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

5. *June 13, Boston Globe Online* — **Logan getting weapons upgrade. Submachine guns, long a common sight in many European airports, made their debut yesterday at Logan Airport, which has spent more than 11/2 years bolstering its security and image after becoming the takeoff point for two of the planes hijacked by terrorists in the September 11 attacks.** Massport purchased 30 of the submachine guns, at a cost of $2,500 each, deploying them with the new State Police antiterrorism unit and making Logan the first airport in the nation to bring such high−tech weaponry to its terminals, roadways, curbs, and ramps. **Each MD5SD weighs 7 pounds and has a long, built−in silencer that the manufacturer says is designed to be so effective that the sound of the bullet firing will make less noise than the clicking of the firing mechanism.**
Source: http://www.boston.com/dailyglobe2/164/metro/Logan_getting_weapons_upgrade+.shtml

6. *June 12, CNN* — **Explosive found on Italian plane. A search of an Alitalia passenger plane at the airport in the town of Ancona has turned up an object that apparently contained explosive material, police say.** In a news release Thursday, the Ancona police said they received an anonymous call shortly after 2:30 p.m. (9:30 a.m. EDT) alerting them to search the plane, which was due to depart for Rome at 3 p.m. from Ancona's tiny airport 300 kilometers (200 miles) east of the capital, on the Adriatic coast. **"We found a suspicious object that later proved to have contained explosive material," the release said. The object, found beneath a seat, was taken from the Aerospatiale ATR−42 and detonated; tests of the residue indicated it had contained an explosive, police said.** No passengers had boarded the plane at the time the device was found, the release said. But the plane was booked near capacity, a reservations clerk told CNN. Depending on its configuration, the propeller plane can carry 42 to 50 passengers. **An Italian wire service described the object as the size of a package of cigarettes, with electric cables attached.** The flight had arrived from Rome earlier in the day, said Alitalia spokeswoman Marta−Marie Lotti, in New York. "As far as Alitalia is concerned, we don't know what objects were found," she said.
Source: http://www.cnn.com/2003/WORLD/europe/06/12/italy.planebomb/i ndex.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

7. *June 16, Associated Press* — **Kansas to test animal disease preparedness.** State officials will spend two days next week finding out just how prepared Kansas is to address an agroterrorism event. **On Wednesday and Thursday, the state emergency operations center will be buzzing with activity as Kansas tests its command and control capabilities during a simulated attack of a foreign animal disease on the state's livestock herds.** The scenario has been developed by the National Agriculture Biosecurity Center at Kansas State University. Participants will include county, state, and federal agencies, as well as representatives from the livestock industry. With more than 10 million animals and $10 billion economic impact, an outbreak of a foreign animal disease in Kansas would be devastating to the Kansas economy. **Kansas has been active in recent years to gird against agroterrorism, including passage of legislation making it a felony to intentionally introduce a plant or animal pathogen. Maj. Gen. Greg Gardner, state adjutant general and director of emergency management, said legislators also took steps to expand the governor's ability to manage a terrorist event.**
Source: http://www.kansascity.com/mld/kansascity/news/local/6079166. htm

[Return to top]

Food Sector

8.

June 12, U.S. Department of Agriculture — **Alabama firm recalls chicken. ConAgra Poultry Company, an Athens, GA, establishment, is voluntarily recalling approximately 129,000 pounds of fresh chicken that may contain glass, the U.S. Department of Agriculture's Food Safety and Inspection Service announced Thursday.** The company is asking distributors in Florida, Georgia, New York, North Carolina, and South Carolina to return 3.5 to 4−pound bags of "Country Pride Fresh Chicken" packages.
Source: http://www.fsis.usda.gov/oa/recalls/prelease/pr027−2003.htm

[Return to top]

Water Sector

9. *June 12, Associated Press* — **New Mexico drought emergency continues.** Governor Bill Richardson has declared a drought emergency that makes New Mexico eligible for federal financial help and continues an order last year by his predecessor, Governor Gary Johnson. **"Despite recent rains, New Mexico continues down a path toward a long−term drought," Richardson said Wednesday.** The state reached agreement with Texas in April that allows some water to be released this year from Elephant Butte reservoir in exchange for the right to store that water in upstream, drought−depleted areas. **Richardson also formed a task force to recommend ways to mitigate drought conditions. It will consider proposals made last year, including local conservation ordinances, water construction projects, and fire prevention efforts.**
Source: http://story.news.yahoo.com/news?tmpl=story_p_on_re_us/brf_new_mexico_drought_3

[Return to top]

Public Health Sector

10. *June 13, Associated Press* — **Two Wisconsin health workers may have monkeypox. Officials are investigating whether two Wisconsin health care workers may have contracted monkeypox from patients, in what would be the first known transmission of the virus from one human to another in the U.S.** Until now, health officials investigating the weeklong outbreak in the United States have said that the virus was being spread by pet prairie dogs. But the disease can also be transmitted from one person to another, something that has happened in Africa. **Patrice M. Skonieczny, infection control coordinator at St. Francis Hospital in Milwaukee, said a nurse developed monkeypox symptoms after caring for a patient with a possible case of the disease. Skonieczny said the nurse at St. Francis was wearing protective clothing, including a mask, gloves and a gown, when she cared for the pet distributor being treated for possible monkeypox.** In another case, Dr. John Melski, a dermatologist at Marshfield Clinic in Marshfield, said a medical assistant is suspected of getting the disease after helping treat a 3−year−old girl May 22.
Source: http://www.washingtonpost.com/wp−dyn/articles/A54341−2003Jun 13.html

11. *June 13, BBC News* — **Drug hope for SARS. Researchers in Germany have identified an existing anti−viral drug which might be used to treat Severe Acute Respiratory Syndrome (SARS). Scientists from the Frankfurt Medical School say tests show a drug called**

Glycyrrhizin is effective against the virus suspected of causing SARS. There are indications that the SARS epidemic, which has infected more than 8,000 people around the world, could be over without the need for drugs. The World Health Organization says the SARS epidemic may be nearing its end, with a decline in the number of new cases appearing each day. **The German scientists say the drug Glycyrrhizin significantly reduces the ability of the virus that causes SARS to replicate itself.** Glycyrrhizin is manufactured from the roots of the liquorice plant and is already used to treat hepatitis C and HIV infections. However, the scientists say they do not understand exactly how the drug combats SARS.
Source: http://news.bbc.co.uk/2/hi/asia−pacific/2986512.stm

12. *June 13, Federal Computer Week* — **CDC overhauling Web site. The U.S. Centers for Disease Control and Prevention (CDC) is redesigning its Web site to allow for easier access to information, reflecting the agency's increased visibility to the public.** "The Web is our face," said Jason Bonander, a lead information technology specialist at CDC. "It's imperative that we continue to evaluate what our needs are." **The CDC historically has been a wholesaler of information, Bonander said, providing statistics and reports primarily to the medical community. In the past two years, the agency has changed into a retailer of information, also providing up−to−date general information to the public, which requires a site that is readable and searchable in different languages and in understandable terms.** "We still need to package information for our public health partners, but we also need to provide information to the public," he said. **For example, during the April outbreak of Severe Acute Respiratory Syndrome (SARS), CDC's Web site received 17.5 million visitors, compared with 5.4 million visitors in all of fiscal 2002. During the anthrax attacks in October 2001, the site saw 9.1 million visitors.**
Source: http://www.fcw.com/fcw/articles/2003/0609/web−site−06−13−03. asp

13. *June 12, Global Security Newswire* — **Monkeypox outbreak tests bioterrorism response systems. U.S. efforts to prepare for a bioterrorist attack have enabled an effective response to this month's outbreak of monkeypox in the U.S., according to health officials and public health experts.** "State health departments have been actively involved in planning and preparing for the possibility of a bioterrorist event. We are now seeing that this level of preparation can also assist in unexpected, natural outbreaks," said Health and Human Services Secretary Tommy Thompson. "Mother Nature has given us a little practice opportunity," said Shelley Hearne, executive director of Trust for America's Health, a nonpartisan public health group. **Hearne compared the monkeypox response to the confused public health reaction during the anthrax mailings of 2002 and said there has "certainly been significant improvement. That's the good news."** She cautioned, however, that the government might be focusing too heavily on a few, select biological threats. "Surveillance has certainly been upgraded," said Von Roebuck, a spokesman for the U.S. Centers for Disease Control and Prevention. "I suspect we may have seen monkeypox in the past and we didn't pick it up," Hearne said. **Enhanced communication in the public health community was the most valuable improvement cited by several officials and experts.**
Source: http://www.nti.org/d_newswire/issues/2003/6/12/7s.html

[Return to top]

Government Sector

14. *June 14, New York Times* — **Senators' bill to ensure E911 funds.** Sens. Conrad Burns (R−MT) and Hillary Rodham Clinton (D−NY) are introducing a bill aimed at keeping state governments from raiding funds dedicated for emergency 911 systems. The bill also would establish a federal interagency committee to help coordinate Enhanced 911 (E911) activities with homeland security and other priorities. **In recent months, advocates and lawmakers supporting E911 have testified several times on Capitol Hill that states have siphoned away money earmarked for cities and emergency dispatch centers, commonly known as Public Safety Answering Points (PSAPs).** Landline and wireless customers pay a small surcharge on their telephone bills, and the collected funds are supposed to go toward improving 911 services. However, because many state governments are grappling with huge budget deficits, some have been dipping into E911 funds.
Source: http://www.fcw.com/geb/articles/2003/0609/web−e911−06−12−03. asp

15. *June 13, U.S. Department of Homeland Security* — **Homeland Security Advisory Council meeting − June 30, 2003 .** The Homeland Security Advisory Council (HSAC or Council) will hold its inaugural meeting on Monday, June 30, 2003 in Washington, DC. **The HSAC will meet for the purposes of: (1) Welcoming and introducing the members of the Council; (2) announcing the Chairs and Vice Chairs of the HSAC's Senior Advisory Committees; (3) receiving briefings by senior government officials on the Department's TOPOFF II exercise; and (4) holding roundtable discussions with and among Council members.** This meeting will be partially closed; the open portion of the meeting, for purposes of (1), (2), and (3) above will be held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue, NW., from 10 a.m. to 12:15 p.m. The closed portion of the meeting, for purposes of (4) above, will be held at the Renaissance Mayflower Hotel from 12:30 to 3 p.m. Due to limited availability of seating, members of the public will be admitted on a first−come, first−served basis. In addition, due to security concerns, any member of the public who wishes to attend the meeting must provide his or her name, social security number and date of birth no later than 5 p.m. EDT, Wednesday, June 25, 2003, to Mike Miron, member of the HSAC staff, via email at HSAC@dhs.gov, or via phone at (202) 786−0279.
Source: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03−15089.htm

16. *June 12, Federal Computer Week* — **DHS seeking alert system.** The Department of Homeland Security (DHS) is putting together a business case for the fiscal 2005 budget that would finance an alert system for the public. Rosita Parks, the chief information officer at DHS' Federal Emergency Management Agency, said on Thursday that the agency is taking an inventory of what technology it has and what kinds of alert systems it could use to warn the public of an emergency. **Ideas being considered include using the National Oceanic and Atmospheric Administration's Weather Radio, currently being developed, and leveraging the text messaging available on some cell phones. "We are proposing a business case to ensure that we are addressing this as a coordinated effort," Parks told a gathering at the E−Gov conference in Washington, DC, sponsored by FCW Media Group.**
Source: http://www.fcw.com/fcw/articles/2003/0609/web−dhs−06−12−03.a sp

[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information and Telecommunications Sector

17. *June 14, ComputerWeekly.com* — **Cybercorps to boost U.S. federal IT security. IT security at U.S. federal agencies will get a boost this month from the first class of 46 students who have completed training under a federal scholarship−for−service program.** Cybercorps was created in 2000 to produce a pool of security−trained IT professionals obligated to work for the U.S. government. The program provides up to two years of scholarship funding for students studying information security in return for a commitment to work an equal amount of time for the federal government. The graduates, about half of whom come from private−sector jobs, were trained at some of the 36 participating colleges and universities. **The Cybercorps program is part of the national plan for information systems protection developed by the Bush administration.**
Source: http://www.computerweekly.com/articles/article.asp?liArticleID=1225461iChannelID=22FlavourID=1

18. *June 13, Federal Computer Week* — **DoD moving to IPv6. Beginning in October, all Defense Department assets acquired for the Global Information Grid (GIG) must be compatible with the next−generation Internet Protocol Version 6 (IPv6),** according to DoD's top information technology official. The GIG is a massive DoD network designed to connect warfighters anywhere in the world. Moving to IPv6 will help the department achieve its goal of network−centric warfare and operations by the end of the decade, said John Stenbit, assistant secretary of Defense for networks and information integration. **Stenbit signed a policy memorandum June 9 that outlines DoD's transition to the new protocol by 2008.** That year was chosen because most experts estimate widespread commercial adoption will take place from 2005 to 2007, he said.
Source: http://www.fcw.com/fcw/articles/2003/0609/web−dodip−06−13−03 .asp

19. *June 13, The Mercury News (CA)* — **Hacker sentenced for breaching Eglin AFB, Sandia lab. An 18−year−old hacker who breached computers at Sandia National Laboratories and posted an anti−Israeli message on the Eglin Air Force Base Web site was sentenced Thursday to a year and a day in federal prison.** Adil Yahya Zakaria Shakour also was ordered to pay $88,253 in restitution, and his computer use was restricted during the three years he will spend under supervised release after his prison term. Shakour, a Pakistani national who lives in Los Angeles, pleaded guilty in March to computer and credit card fraud charges. **Shakour penetrated the Florida air base's computer server repeatedly in April and May 2002, altering the Web page to denounce the Israeli advance into Palestine. Damage to the air base computer system was estimated at $75,000, while more than $2,700 in damage was done to the Sandia Laboratories Web site.**
Source: http://www.siliconvalley.com/mld/siliconvalley/news/6079276. htm

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 80 (www), 1434 (ms−sql−m), 445 (microsoft−ds), 139 (netbios−ssn), 4662 (eDonkey2000), 0 (−−−), 25 (smtp), 2234 (directplay), 113 (ident) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

20. *June 15, Associated Press* — **Man accused of Grand Coulee Dam threats.** An eastern Washington man has been arrested on federal charges accusing him of threatening to blow up Grand Coulee Dam. **Richard Vialpando, 40, is charged with nine counts of maliciously conveying false bomb threats. He was arrested Friday at his home in Othello, about 100 miles southwest of Spokane, and ordered held without bail. A federal indictment accuses him of making telephone threats between Aug. 21, 2001, and Feb. 5, 2002, that targeted Grand Coulee Dam, the lake behind it and a marina, as well as offices for the FBI and U.S. Secret Service in Washington state.** Other federal officials familiar with the case told The Spokesman−Review there was no evidence suggesting Vialpando had any ties to terrorist organizations.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−brf−bomb−threats,0,1503204.story?coll=sns−ap−nation−headlines

21. *June 14, New York Times* — **Police in Thailand seize radioactive material.** Authorities in Thailand, acting on information from American investigators, seized a large amount of radioactive material from a Thai man, breaking up a plot to sell it to terrorists. He was peddling it for use in so−called dirty bombs, according to American law enforcement officials. American officials said the seized material − which Thai authorities said was cesium−137, a radioactive byproduct of nuclear power plants commonly found in medical equipment − was believed to have originated in Russian stockpiles and been taken to Thailand via Laos. It could easily have been used in terrorist weapons, the officials added. **Law enforcement officials and terrorism experts said they were alarmed that so much of the material − as much as 66 pounds, according to initial reports − was apparently available for sale on the black market. Even a "dirty" bomb with only a few grams of cesium would be deadly, the experts said. It is**

particularly troubling that the material turned up in Thailand, which Al Qaeda has long used as a hub in Southeast Asia, they said.
Source: http://www.nytimes.com/2003/06/14/international/asia/14NUKE. html

22. *June 14, Reuters* — **Saudi says arrests five more Riyadh blast suspects.** Saudi Arabia has arrested five more suspects in suicide bomb blasts which killed 35 people last month, Interior Minister Prince Nayef was reported on Saturday as saying. Four of them were arrested during recent security checks, he told the al−Riyadh newspaper. ``They were part of the group but their roles are not clear yet, while there's a fifth who was arrested before that who might have had a major role," he added. **Prince Nayef said the five men, whose nationalities he did not mention, were in addition to 25 people already in detention over the attacks, in which armed assailants drove into the compounds for expatriates and set off huge car bombs.** Saudi Arabia last week announced the names of 12 Saudi nationals who it said were the suicide bombers who carried out the May 12 attacks, which have been blamed on Saudi−born Osama bin Laden's al Qaeda network.
Source: http://www.nytimes.com/reuters/news/news−saudi−arrests.html

23. *June 10, Deutsche Welle* — **U.S. and EU reach terrorism accord.** A legal cooperation deal between the European Union and the United States worked out in secret over the past year is due to be signed in the coming weeks. **In an effort to smooth cooperation between the two sides, the pact, which has been under negotiation by justice and home affairs ministers in the 15−member union since the summer, will replace bilateral agreements currently in effect between the United States and countries like Germany and Britain.** Officials on both sides of the Atlantic praised what is being seen as a shining example of cooperation in one of the few areas where Europe and the United States work together in harmony.
Source: http://www.dw−world.de/english/0,3367,1430_A_890200_1_A,00.h tml

24. *June 09, National Post* — **RCMP hunting for those tied to 9/11, secret report says.** The Royal Canadian Mounted Police (RCMP) has launched "several solid investigations" into Islamic terrorist activity in Canada as a result of information obtained since the 9/11 attacks, according to a newly declassified RCMP report. "In the immediate aftermath of the September 11 attacks in the U.S., the RCMP saw a massive amount of information concerning Islamic terrorists pour in," says the report, dated October 11, 2002. **"The vast majority of it proved to be unfounded or inconsequential, yet requiring investigation. A year later, we have several solid investigations underway and many resources committed to assisting U.S. authorities track down those connected to the attacks."** Political leaders in Ottawa have consistently denied there was any Canadian link to the September 11 attacks. But while none of the 19 hijackers came from this country, dozens of members of Osama bin Laden's al Qaeda network have used Canada as a base.
Source: http://www.nationalpost.com/national/story.html?id=4F895758−6E17−46A9−B575−E9ADF0EC306B

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer